(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
08 February 2018 (08.02.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/026290 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/NZ2017/050108

(22) International Filing Date:
04 August 2017 (04.08.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
722960 05 August 2016 (05.08.2016) NZ

(71) Applicant: **AUCKLAND UNISERVICES LIMITED** [NZ/NZ]; Level 10, 70 Symonds Street, Auckland, 1010 (NZ).

(72) Inventors: **ASGHAR, Muhammad Rizwan**; 484 Hillsborough Road, AUCKLAND, 1041 (NZ). **HU, Qinwen**; 23A Felton Mathew Avenue, St Johns, AUCKLAND, 1072 (NZ). **BROWNLEE, John Nevil**; 161 Remuera Road, AUCKLAND, 1050 (NZ).

(74) Agent: **BALDWINS INTELLECTUAL PROPERTY**; PO Box 5999, Wellesley Street, Auckland, 1010 (NZ).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: CERTIFICATE REVOCATION SYSTEM

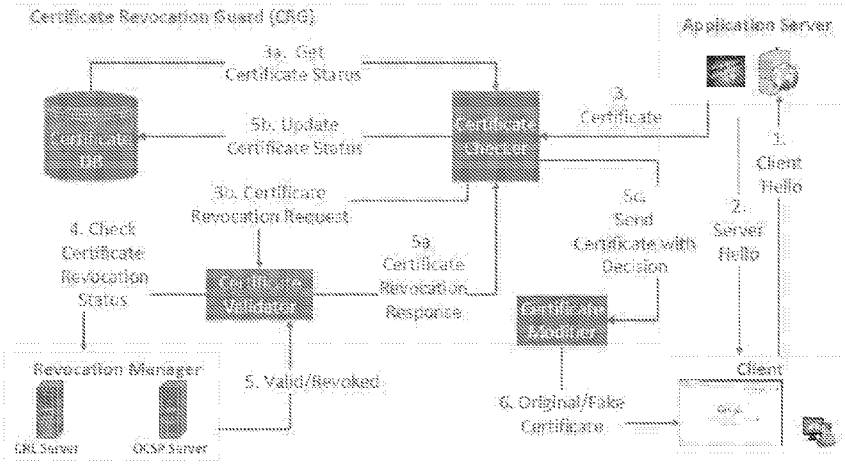

Figure 3

(57) Abstract: A certificate revocation system for checking the validity of digital certificates in a secure online channel where there is a certificate authority capable of issuing a digital certificate to an application server. The system has a certificate checker and a certificate validator to check the status of the digital certificate. When the status returns "valid" a certificate modifier sends a validated certificate to the client, and when said status returns "revoked" a certificate modifier sends a fake certificate to the client, such that validation at the client will fail.

WO 2018/026290 A1

CERTIFICATE REVOCATION SYSTEM

Field of the Invention

The present invention relates to a certificate revocation method and system that efficiently checks certificate revocation while minimising bandwidth, latency and storage overheads.

Background

Online transactions are becoming more ubiquitous nowadays. In today's Public Key Infrastructure (PKI), the Secure Socket Layer (SSL) or Transport Layer Security (TLS) is the most widely deployed protocol for securing online communication. It offers mutual authentication and establishes a secure channel for providing encryption for end-to-end communication over the Internet. There is a wide range of services that use SSL/TLS, such as secure web browsing (i.e., HTTPS), secure virtual communication (i.e., VPNs) and secure file transfer (i.e., SFTP).

The SSL/TLS protocol is based on certificate validation, which takes place before establishing a secure channel between two entities. This validation fails if any certificate in the certificate chain (involving root, intermediate and leaf) is revoked, which could be due to compromised or stolen private keys or fraudulent issuance. If not revoked properly, a leaf certificate can enable attackers to easily eavesdrop the communication until the certificate is expired. The situation is even worse when it comes to an intermediate (or root) certificate because it allows attackers to issue 'valid' certificates for any domains. Therefore, it is essential to check certificate revocation during the certificate validation process.

There are two commonly used methods to check certificate revocation, namely Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). The CRL method allows clients to fetch a list of revoked certificates while the OCSP method responds with the status of a certificate when requested. There is also an extension of OCSP, called OCSP Stapling, which allows clients to pull the revocation status from the application server instead of the OCSP server, thus reducing network latency by saving an extra round-trip.

Most recent studies "Measuring the latency and pervasiveness of TLS certificate revocation," L. Zhu, J. Amann, and J. S. Heidemann, in Passive and Active Measurement - 17th International Conference, PAM 2016, Heraklion, Greece, March 31 - April 1, 2016, Proceedings, 2016, pp. 16–29 and "An end-to-end measurement of certificate revocation in the web's PKI," Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A.

Schulman, and C. Wilson, in Proceedings of the 2015 ACM Conference on Internet Measurement Conference, ser. IMC '15. New York, NY, USA: ACM, 2015, pp. 183–196 have shown that many web browsers do not use the recommended methods for checking certificate revocation. The main reason behind that could be bandwidth overhead, network latency, storage overhead or even privacy risks. Unfortunately, bypassing the certificate revocation check can result in session hijacking and unauthorised issuance of new certificates.

Over the last two decades, there has been a lot of work on the effectiveness of certificate revocation and associated privacy concerns. In "Towards short-lived certificates," E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh, Web 2.0 Security and Privacy, 2012, Topalovic et al. suggested to have short-lived certificates. However, this design results in high bandwidth overheads due to the inconvenience of fetching new certificates valid only for a short span of time. In "On certificate revocation and validation," P. C. Kocher, in Financial Cryptography. Springer, 1998, pp. 172–177, Kocher proposed a tree-based approach for checking certificate revocation, requiring high computational cost at the client end. There are also some other solutions but most of those solutions "Fast digital identity revocation," E. N. Ed, W. Aiello, S. Lodha, and R. Ostrovsky, in 18th Annual International Cryptology Conference (CRYPTO98). Springer-Verlag, 1998, pp. 137–152, "Generalized certificate revocation," C. A. Gunter and T. Jim, in Proceedings of the 27th ACM SIGPLAN-SIGACT symposium on Principles of programming languages. ACM, 2000, pp. 316–329, "Reducing certificate revocation cost using NPKI," A. Levi and C. K. Koc¸, IEEE Journal on Selected Areas in Communications, vol. 18, pp. 561–570, 2000, "PKI Safety Net (PKISN): Addressing the Too-Big-to-Be-Revoked Problem of the TLS Ecosystem," P. Szalachowski, L. Chuat, and A. Perrig, arXiv preprint arXiv:1601.03874, 2016 and "PKI: it's not dead, just resting," P. Gutmann, Computer, vol. 35, no. 8, pp. 41–49, August 2002 require changes in the legacy infrastructure.

There are a number of studies, such as "An efficient authentication scheme to protect user privacy in seamless big data services," Y.-S. Jeong and S.-S. Shin, Wireless Personal Communications, vol. 86, no. 1, pp. 7–19, 2015 and "Analyzing android encrypted network traffic to identify user actions," M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, IEEE Trans- actions on Information Forensics and Security, vol. 11, no. 1, pp. 114– 125, January 2016, showing that many applications (such as online banking apps, VPNs, and web browsers) use SSL/TLS for establishing a secure channel to exchange sensitive information. The main goal of this secure channel is to offer mutual authentication and preserve integrity and confidentiality of exchanged information. Basically, SSL/TLS allows clients to verify

identity of the target server before establishing the private communication. SSL/TLS falls under PKI, which we briefly discuss below.

Digital Certificate

A digital certificate is used as a key component that binds a subject's ID to its public key. It consists of a number of fields including, but not limited to: the subject's name; the subject's public key; the certificate issuer, a.k.a. the Certificate Authority (CA), an authorised entity that issues digital certificates; a serial number that uniquely identifies the digital certificate; validity period indicating start and expiration dates of the certificate; a certificate chain, building a chain of certificates up to the root CA, which is a trust anchor (a list of trust anchors is shipped with Operating Systems (OS)) in the PKI model; typically, there are three types of digital certificates: a leaf, an intermediate and a root, where the latter two types are part of the certificate chain; and information about the authority that manages revocation information.

Certificate validation is an essential part of SSL/TLS. While validating a certificate, it is also important to check certificate revocation. Basically, a certificate might need to be revoked before its expiry if the private key corresponding to the certificate is compromised or stolen. If not revoked properly, leaf and intermediate certificates with compromised/stolen private keys can result in session hijacking and unauthorised issuance of new certificates, respectively.

There are two commonly used methods for disseminating information about certificate revocation: CRL and OCSP. Ideally, as part of certificate validation, the certificate revocation status must be checked.

Figure 1 illustrates the model and visualises the problem. Here, a CA issues a certificate to an Application Server (Step I). If requested, the CA can revoke an issued certificate and publishes a CRL (Step II), which is managed by the Revocation Manager. In our model, we assume that the revocation manager manages both a CRL server and an OCSP server.
In Figure 1, dotted lines represent the certificate issuance and revocation workflow while solid lines show the sequence of establishing the SSL/TLS connection. In SSL/TLS, a Client (i.e., a web browser) sends a Client Hello message (Step 1) to request a new SSL/TLS connection. The application server responds with a Server Hello message (Step 2) followed by a server Certificate (Step 3). After receiving a certificate, the client validates the certificate.

However, as reported by some studies "An end-to-end measurement of certificate revocation in the web's PKI," Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, in Proceedings of the 2015 ACM Conference on Internet Measurement Conference, ser. IMC '15. New York, NY, USA: ACM, 2015, pp. 183–196 and "Analysis of SSL certificate reissues and revocations in the wake of heartbleed," L. Zhang, D. Choffnes, D. Levin, T. Dumitras, A. Mislove, A. Schulman, and C. Wilson, in Proceedings of the 2014 Conference on Internet Measurement Conference, ser. IMC '14. New York, NY, USA: ACM, 2014, pp. 489–502, some clients miss the certificate revocation check as we can see in Figure 1.

Certificate Revocation Lists (CRLs)

A Certificate Revocation List contains a list of revoked certificates, each CRL entry represents a serial number, a revocation timestamp and a revocation reason (optional) for the revoked certificate. In this method, CAs embed the CRL's URL in each released certificate, which can be downloaded by the client. The CRL file helps the client to check whether the current certificate's serial number is listed in that CRL. Every CRL has an expiration date that allows the client to cache the CRL file until it expires. This method requires CAs to periodically re- issue a new CRL, even if it is not updated. If the cached CRL expires, the clients must download an updated CRL file. The major limitations of this method include high bandwidth, network latency and storage overheads for the client.

Online Certificate Status Protocol (OCSP)

As an alternative solution to CRLs, OCSP reduces bandwidth and storage overheads by allowing clients to query an OCSP server for the revocation status of a single certificate. Similar to CRLs, the OCSP server's URL can be found in the issued certificates. The client sends an HTTP GET request to the OCSP server for querying the status of the given certificate. There are three different types of OCSP status responses: good, reject and unknown, indicating that a certificate is not revoked, it is revoked or the OCSP server does not know about the certificate being requested. This method has its own drawbacks. The client queries the certificate revocation status every time instead of caching the list of revoked certificates, thus increasing the latency as well as privacy risks.

There is also an extension of OCSP that allows clients to directly get the certificate status from the application server. This new method is called OCSP Stapling, see "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension," Y. Pettersen, IETF RFC 6961, 2013, in which the application server queries the OCSP server and caches the status of its own certificate. The OCSP stapling method solves the privacy issue in OCSP and

reduces the latency. However, this extension is not supported by all the servers. Second, this extension still increases some bandwidth and latency because an application server has to send the OCSP status to the client, which verifies that OCSP status.

Summary of Invention

The present invention may broadly be said to consist in a certificate revocation system for checking the validity of digital certificates in a secure online channel where there is a certificate authority capable of issuing a digital certificate to an application server, the application server capable of communicating the digital certificate to a client, the system comprising:

a) a certificate checker to intercept a certificate message from the application server to the client and to forward a certificate revocation request to a certificate validator,
b) a certificate validator to check the status of the digital certificate in the certificate message with the revocation manager,
c) and when said status returns “valid” a certificate modifier sends a validated certificate to the client,
d) and when said status returns “revoked” a certificate modifier sends a fake certificate to the client, such that validation at the client will fail.

Preferably after the certificate checker intercepts the certificate message, the certificate checker consults the certificate database before forwarding a certificate revocation request to a certificate validator.

Preferably the system includes caching the returned statuses, either “valid” or “revoked” in a certificate database.

Preferably the certificate validator requests the certificate status, gets the status and sends the response to the certificate checker.

Preferably the certificate checker updates the certificate database and forwards the decision together with the digital certificate to the certificate modifier, which can send the original or fake certificate to the client.

Preferably at interception of the certificate message by the certificate checker the certificate checker extracts the serial number of the digital certificate.

Preferably when the certificate modifier creates a fake certificate, the fake certificate is a modified version of the original digital certificate.

Alternatively the fake certificate is a precomputed fake certificate stored at the certificate modifier.

The disclosed subject matter also provides method or system which may broadly be said to consist in the parts, elements and features referred to or indicated in this specification, individually or collectively, in any or all combinations of two or more of those parts, elements or features. Where specific integers are mentioned in this specification which have known equivalents in the art to which the invention relates, such known equivalents are deemed to be incorporated in the specification.

Further aspects of the invention, which should be considered in all its novel aspects, will become apparent from the following description.

Drawing Description

A number of embodiments of the invention will now be described by way of example with reference to the following drawings.

Figure 1 is a certificate revocation system of the prior art, and in particular of a PKI model indicating certificate issuance and revocation as well as showing SSL/TLS certificate exchange and validation.

Figure 2 is an illustration of the certificate revocation system of the present invention in which there is an interception of an SSL/TLS certificate message (Step 3) and consultation of the certificate revocation status with a revocation manager (Step 4). Preferably the system caches the response (Step 5) and, depending on the valid or revoked certificate, sends either an original or a fake certificate (Step 6) to the client, respectively.

Figure 3 is a detailed view of certificate revocation system of the present invention. Here in case of a new certificate, a certificate checker intercepts the SSL/TLS certificate message (Step 3), consults the certificate database (Step 3a) before forwarding a certificate revocation request to a certificate validator (Step 3b). The certificate validator requests the certificate status (Step 4), gets the status (Step 5) and sends the response to the certificate checker (Step 5a). The certificate checker updates the certificate database and forwards the

decision together with the certificate (Step 5c) to the certificate modifier, which can send an original or fake certificate to the client (Step 6).

Figure 4 is a summary of data used for experiments, particularly showing how many unique as well as total requests were received.

Figure 5 is a graph showing a comparison of bandwidth overheads of two existing methods with the certificate revocation system of the present invention. The graph shows that the system of the present invention saves over 95% bandwidth cost when compared with OCSP.

Figure 6 is a graph showing a comparison of network latency of two existing methods with the certificate revocation system of the present invention. As compared to OCSP, the system of the present invention improves latency by 95%.

Figure 7 is a graph showing a comparison of local disk storage between the certificate revocation system of the present invention and CRL. The system of the present invention saves storage space by 69%.

Detailed Description of the Drawings

Throughout the description like reference numerals will be used to refer to like features in different embodiments.

In Public Key infrastructure (PKI) models, digital certificates play a vital role in securing online communication. Communicating parties exchange and validate these certificates and the validation fails if a certificate has been revoked. The inventors have devised a certificate revocation system that efficiently checks certificate revocation while minimises bandwidth, latency and storage overheads. The system is based on OCSP, which caches the status of certificates locally. The system may be installed on the user's machine, at the organisational proxy or even at the ISP level. Compared to a naive approach (where a client checks the revocation status of all certificates in the chain on every request), the system of the present invention decreases the bandwidth overheads and network latencies by 95%. Additionally, using the system of the present invention incurs 69% lower storage overheads compared to the CRL method. The results from tests and experiments demonstrate the effectiveness of the system to improve certificate revocation.

The certificate revocation system of the present invention is based on OCSP and caches the certificate revocation status locally. As such it takes advantages of both OCSP and CRL methods. It saves bandwidth cost, network latency and storage cost when compared with

OCSP and CRL. Additionally, certificate revocation system of the present invention does not require any changes in the legacy infrastructure and can be installed on the user's machine, at the organisational gateway/proxy or even at the ISP level.

In the PKI model, digital certificates play a vital role in securing the online communication. Before establishing a secure channel, communicating parties exchange and validate these certificates. Certificate validation fails if the certificate is revoked, which could be due to compromised or stolen private keys or fraudulent issuance. There are commonly used methods to check certificate revocation, namely CRL and OCSP.

However, recent studies "An end-to-end measurement of certificate revocation in the web's PKI," Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, in Proceedings of the 2015 ACM Conference on Internet Measurement Conference, ser. IMC '15. New York, NY, USA: ACM, 2015, pp. 183–196 and "Analysis of SSL certificate reissues and revocations in the wake of heartbleed," L. Zhang, D. Choffnes, D. Levin, T. Dumitras, A. Mislove, A. Schulman, and C. Wilson, in Proceedings of the 2014 Conference on Internet Measurement Conference, ser. IMC '14. New York, NY, USA: ACM, 2014, pp. 489–502 show that clients do not check revocation status as part of certificate validation (as illustrated in Figure 1). The main reasons could be privacy risks or bandwidth/storage and latency overheads associated with checking certificate revocation "Towards short-lived certificates," E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh, Web 2.0 Security and Privacy, 2012. Unfortunately, missing the certificate revocation check can result in session hijacking or unauthorised generation of new certificates.

The major issue with CRL is its high bandwidth, storage and latency overheads. OCSP partially solves this problem by allowing clients to query an OCSP server for the revocation status of a single certificate. However, the OCSP method is not only privacy invasive but also incurs high latency and bandwidth overheads. To solve the privacy issue, there is also an extension of OCSP, OCSP stapling, which allows clients to query the certificate status from the application server, which caches the status of its own certificate. However, this extension is not supported by all the servers. In short, all the certificate revocation methods suffer from at least one of the following issues: privacy invasive, high latency, high bandwidth and storage overheads.

Certificate revocation is not widely used today because the existing methods fail to meet the privacy and performance requirements. The certificate revocation system of the present invention, herein referred to as "Certificate Revocation Guard (CRG)", aims at addressing

the problems associated with CRL and OCSP methods. The basic workflow of CRG is outlined in Figure 2. As we can see, both certificate issuance (Step I) and CRL publication (Step II) stay the same. That is, we do not require any modification in the SSL/TLS protocol so Steps 1, 2 and 3 are the same as already illustrated in Figure 1. However, CRG intercepts the certificate message of the SSL/TLS protocol (Step 3) and consults its status with the revocation manager (Step 4), which returns either valid or revoked (Step 5). If the status is valid, CRG sends (Step 6) the original certificate it received in Step 3. If the certificate has been revoked then CRG has to communicate this information to the client. It is important to mention that the underlying protocol between the client and the application server is not modified. Instead, a fake certificate is generated to indicate that the certificate is not valid anymore. In other words, the fake certificate is such that its validation on the client will fail.

Figure 3 provides a detailed view of CRG. Figure 3 shows that CRG is decomposed into four main components: a certificate checker, certificate database, certificate validator and certificate modifier. From the deployment point of view, CRG could be installed on the user's machine, at the organisational proxy or even at the ISP. Each deployment choice has possible trade-offs that are discussed in detail below. The functionality of each entity is described below.

Certificate Checker

We define the certificate checker as a core component in the system. It is an interface between the application server and rest of the components in CRG. It is responsible for intercepting the SSL/TLS certificate messages. After intercepting a certificate message, for each certificate in the certificate chain (except root certificates), it checks performance based on the certificate's serial number, which is extracted by the certificate checker. For each certificate, there are two possibilities: either the certificate is an existing one, meaning its status was already cached recently or it is a new certificate (or an existing one with expired caching time, which is explained later). The former case saves CRG bandwidth and reduces the latency. Therefore, it first checks with the certificate database. In the latter case, it has to request the certificate validator for checking the revocation status. In either case, it sends the certificate chain together with a revocation decision to the certificate modifier. The decision is considered yes if the status of all the certificates in the certificate chain is valid. Otherwise, the decision will be no.

Certificate Database

The certificate database creates and manages the revocation information for each requested certificate. For each certificate entry, the database maintains the following fields: the certificate's serial number, the revocation status, the next update time when the revocation status needs to be checked again, the certificate type, frequency of request (indicating how many times a certificate has been requested) and the certificate issuer as depicted in Table I. We assume that the certificate database is populated based on requests by the certificate checker. From the configuration point of view, CRG is flexible enough. Specifically, it is possible to allocate a certificate database of a certain size. In that case, the certificate database has to be downsized once it approaches the configured size limit. To this end, we have different choices. One straightforward choice is to remove entries with a lower frequency of requests, considering they will not be frequently requested. We can also filter based on certificate type, next update time, revocation status or certificate issuer. In case of filtering based on certificate type, we can remove entries with leaf certificates assuming intermediate certificates will be requested more frequently. Another potentially attractive choice is removing all entries where next update time has been reached (or is about to be reached). Likewise, we can choose either valid or revoked ones. The certificate issuer could be a more personalised choice that takes into account what are typical issuers in the user's vicinity because they have the likelihood to be requested the most. Alternatively, we can consider refreshing the certificate database based on most recently used or less recently used in which case we also need to record the time of the request. Without loss of generality, we can specify a policy that could be based on a set of possible designed choices optionally with complex conditions.

Certificate Validator

The goal of the certificate validator is to check the certificate revocation by contacting the revocation manager. The certificate checker requests the certificate validator by providing information about the authority that manages revocation information, *i.e.,* the revocation manager. After receiving the request, the certificate validator connects with the revocation manager and gets the certificate status, which is either *valid* or *revoked.* It is important to distinguish between two authorities that manage revocation information: a CRL server and an OCSP server. A certificate provides information about at least one of them. Typically, a certificate includes URLs of both servers. Using a CRL server may provide more information than required because the certificate validator will get a list of all the revoked certificates, incurring high bandwidth and storage costs but being more privacy-preserving and efficient from the point of view of caching the complete list for subsequent requests. On the other hand, if we contact the OCSP server, we can lower storage and bandwidth overheads at the cost of increased latencies for subsequent requests.

However, OCSP is less privacy-preserving as the revocation manager would be able to profile behaviour of the client. For efficiency reasons, we use the OCSP method, but we cache the response in the certificate database so that we can minimise potential privacy issues as well as decrease the latency and bandwidth overheads.

Certificate Modifier

The certificate modifier issues a fake certificate if the certificate has been revoked. The fake certificate is specifically designed to signal the client that the certificate has been revoked. A fake certificate can easily be made from the original one by modifying the certificate expiry. Alternatively, we can change other fields (such as signatures) in the certificate that can result in unsuccessful validation. However, the aforementioned approaches of generating fake certificates will result in high latency due to modifications in original certificates. We can follow a radically different approach by pre-computing a set of fake certificates that could be used by the certificate modifier. If the original certificate is valid, the certificate modifier does not take any action and forwards the original certificate to the client.

Experiments

In the following, we discuss three cases indicating three situations: when CRG receives a new certificate, a cached certificate with the next update time reached and a cached certificate without the next update time reached. The two former ones represent the most complex case because in both situations CRG has to contact the revocation manager.

Serial Number	Revocation Status	Next Update Time	Certificate Type	Frequency of Request	Certificate Issuer
123456789	Valid	25/04/2016	Leaf	50	GeoTrust Global CA
345678912	Revoked	28/04/2016	Leaf	40	GeoTrust Global CA
781234567	Valid	30/04/2016	Intermediate	120	GeoTrust Root CA
116890045	Revoked	29/04/2016	Intermediate	100	Baltimore CyberTrust Root
...	...	...	...	...	...

Table 1: An example of a database with cached certificates, each one identified with a serial number, stored with its Revocation status (valid or revoked), next update time

when the revocation manager needs to be contacted again, certificate type (leaf or intermediate), frequency of request and certificate issuer.

Case 1) In case of a new certificate, after receiving the certificate (Step 3), the certificate checker gets the status update from the certificate database (Step 3a). Since the certificate is new, there will be no entry in the database. The certificate checker has to contact the certificate validator (Step 3b). The certificate validator checks the status of this new certificate (Step 4) and gets the response (Step 5), which it forwards back to the certificate checker (Step 5a). To cache the status, the certificate checker updates the database (Step 5b) by inserting a new entry for this new certificate and initialises the frequency of request field with 1. The certificate checker also sends the decision to the certificate modifier (Step 5c). Note that both Steps 5b and 5c can run in parallel. However, for reducing the latency, we recommend Step 5c should take precedence. Based on the decision made by the certificate checker, the certificate modifier finally communicates back to the client (Step 6).

Case 2) If there is a cached certificate with the next update time reached, like the case of a new certificate, CRG performs the same steps (*i.e.,* Steps 3b, 4, 5, 5a and 6) except Step 5b. For updating status of a certificate having an entry in the database with the next time reached, CRG updates its revocation status and next update time as well as incrementing the frequency of request by one.

Case 3) If the certificate is a cached one without the next update time reached, after receiving the certificate (Step 3), the certificate checker gets the status update from the certificate database (Step 3a). Since there is already an entry in the table, it increments the frequency of request by one. Next, it directly sends the response to the certificate modifier (Step 5c), which ultimately forwards the certificate to the client (Step 6).

Extending CRG

In general, CRG is able to efficiently deal with certificate revocation. CRG relies on the assumption that status of a certificate will stay the same until the next update time. The next update time is part of the OCSP or CRL response. However, in practice, the certificate can get revoked before this time.

Therefore, as an option, CRG may subscribe to instant revocation of certificates whenever a new certificate gets cached. This will require the revocation manager to introduce an additional server that is responsible for handling subscriptions. This additional server will

update all subscribers with information about certificates that get revoked before the next update time. The certificate validator on the CRG end can be responsible for dealing with such subscriptions. Since the system of the present invention is flexible, users will be allowed to configure whether this option of CRG with the subscription mode should be on or off. Like the policy for downsizing the certificate database, users can specify a policy for narrowing down a set of certificates which they can subscribe to.

PERFORMANCE ANALYSIS

In this section, we provide a comparative analysis of overheads incurred by existing methods (including CRL and OCSP) and the certificate revocation system of the present invention. Specifically, we analyse network latency as well as bandwidth and storage overheads. Our results show that CRG outperforms both CRL and OCSP methods.

Data Collection

For our experiments, we have collected live Internet traffic (i.e., HTTPS). To collect the data, we have written a Python script of nearly 300 lines of code. We run this script on a monitoring PC at the gateway of The University of Auckland, New Zealand. Using our Python script, we captured and recorded the first three messages (i.e., Client Hello, Server Hello and Certificate) of SSL/TLS flows. The monitoring machine is running Ubuntu on an Intel 6 Xeon E5-2430 2.2 GHz with 32 GB memory. Since the gateway typically processes a huge amount of data, we were able to collect 1.2 GB data just within half an hour. Due to local disk storage limitation, we could not store more data. After the data collection, for running our benchmarking experiments, we used a Windows 7 machine having a Core i5 2.2 GHz processor with 8 GB memory. To extract certificate messages from the trace file, we used TShark2. Each certificate message in the SSL/TLS protocol represents a chain of certificates involving root, intermediate and leaf certificates.

Our results show that there are 2200 SSL/TLS certificate messages in the dataset we used for our experimentation. Figure 4 illustrates breakdowns of root, intermediate and leaf certificates in all the requests. In total, there are 1867 root, 1920 intermediate and 2187 leaf certificates. We discovered that root, intermediate and leaf certificates are repeated on average around 124, 58 and 13 times, considering they uniquely appear 15, 33 and 166 times respectively in our dataset.

In our experiments, we do not consider checking revocation status of root certificates, assuming they are taken care by OS or browsers. Without loss of generality, root certificates can also be handled by our approach.

Bandwidth Cost

Bandwidth refers to the data throughput capacity for each certificate's revocation checking. In case of CRG and CRL, after checking certificate revocation, the client caches the revocation status locally for a certain time. This caching saves bandwidth cost because the client can locally check revocation status of certificates that are repeated. However, OCSP requests the OCSP server to check the revocation status of each certificate, even if the certificate is repeated. For measuring bandwidth overhead, we use the dataset described in above and calculate the accumulative bandwidth cost of all the requests. The comparison of bandwidth has been shown in Figure 5. Our dataset shows that OCSP requires 850 bytes for checking the revocation status. Since CRG is built on OCSP, it also requires 850 bytes for checking the revocation status and the same caching cost, which is explained in Section V-D. CRL uses more bandwidth for fetching the CRL file, the median value of bandwidth usage is 1800 bytes, which is more than double than that of CRG. However, the size of a CRL response is dependent on the number of certificates to be revoked. Therefore, a CRL response can be large, while an OCSP response is always the same size. If we compare CRG with OCSP, we save over 95% bandwidth cost.

Network latency is the time between sending the revocation status request and receiving the response. In our experiments, we observed a network latency from 20 millisecond (ms) to 2 seconds. The average latency for OCSP and CRG is 30 ms. It may take longer for CRL depending on the file size. The median value for latency in case of CRL is 700 ms. Similar to bandwidth cost, we use the dataset described and calculate the accumulative network latency of all the requests. We present results of network latency in Figure 6. Like bandwidth comparison, CRG incurs the low latency overhead because it processes 95% requests locally. In contrast, OCSP incurs the most latency overhead, as it interacts with the OCSP server for each request.

Since we cache the status of revoked certificates that requires some storage. In a CRL file, there is a single entry for each revoked certificate. The file size determines the total number of entries. This is similar to the certificate database in CRG. On average, each certificate entry occupies 300 bytes in CRG. In contrast, most of the CRLs are of 1000 bytes. The difference is caused by the inconsistent CRL file size. Typically, the file includes all the revoked certificates from the same CAs. Liu *et al.* observed that the CRL file size can be up to 51 KB in "An end-to-end measurement of certificate revocation in the web's PKI," Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, in Proceedings of the 2015 ACM Conference on Internet

Measurement Conference, ser. IMC '15. New York, NY, USA: ACM, 2015, pp. 183–196. Conversely, each entry in CRG only contains revocation status of the requested certificates. Figure 7 demonstrates the storage cost for saving revocation status of approximately 200 certificates using CRG and CRL. OCSP is not considered because it does not cache the revocation status. As compared to CRL, CRG saves storage cost by 69%.

Deployment

From the deployment point of view, it is possible to install the certificate revocation system of the present invention on the user's devices or to consider an on-path deployment strategy. The system (CRG) needs to receive each SSL/TLS flow between clients and servers for managing the certificate revocation status. In the following, we discuss possible choices to deploy CRG.

a) Client Side Deployment

Our findings confirm that fetching revocation status can be an expensive operation for clients, particularly those with limited resources. There is a trade- off between the limited storage usage and the low network capacity. For the former, clients have to set a limited size for the certificate database and clear it when it is nearly full. In the latter case, clients can increase the storage usage for caching more OCSP responses. From the communication point of view, all the processes will be handled locally by CRG on the device. Generally, there is no communication cost for checking the cached certificates.

b) Router Deployment

Caching OCSP responses on the router closer to the target networks reduces the latency because the latency depends largely on how far the client is away from the OCSP servers. The drawback of doing this is the storage size because the existing routers have a small storage space for maintaining the routing policy. If we want to deploy CRG on the existing routers, we have to consider the certificate database size. However, placing CRG on the router brings many benefits including improving global availability, reducing bandwidth and no additional upgrading requirements on the client side.

c) Gateway/Proxy Deployment

CRG can be located at the gateway or proxy level. It would help to improve user experience for fetching the certificate revocation status with a lower bandwidth cost and a lower latency. From the management view, this deployment option reduces an operation cost for making any changes in CRG compared to aforementioned ones. Network administrators only modify

CRG at the gate- way/proxy instead of changing all the routers or all the client devices in a target network.

d) ISP Level Deployment

There is no an additional requirement for placing CRG at the ISP level. The only concern is the storage size because the number of cached certificates can become very high by monitoring all certificates from the subscribing networks. Clients have to determine the most effective size of their certificate database.

The database size is the main requirement when deploying CRG in different locations. We suggest clients configure storage size as high as possible in any location to fully exploit potential benefits of CRG.

Increased Performance Gain

In our experiments, due to our disk storage limitation, live traffic only for half an hour only was collected. Based on our sample file, we noticed 94% of requests were using cached certificates. If we extended the measurement time to a week (which is a typical time when the caching status expires) or more, we believe more cached certificates will be observed, thus enabling increased performance gain. Consequently, it will generate better performance results.

Privacy and Security Considerations

a) Minimising Privacy Loss

Privacy has been an issue when we use OCSP because a user's browsing behaviour can be deduced by analysing all OCSP requests. In CRG, we do not interact with OCSP for every request. After making the first request to the revocation manager, the OCSP response is cached fora certain period in which it remains valid, i.e., the next update time. The next request to the revocation manager is sent when the next update time is reached or a new certificate is observed. This design significantly improves the user behaviour visible to the revocation manager.

b) Denial of Services (DoS)

DoS attacks can be mounted to overload the certificate DB or by sending fake requests in an attempt to exhaust the processing resources. For the former case, users can set up a size limitation for the certificate DB. When the certificate DB size limit is reached, CRG will stop caching OCSP responses, however the revocation checking will still work. In this way, we can minimise the risk of DoS and other attacks (such as the memory overloading attack,

which could easily be mounted when the certificate DB size is small and an attacker is able to send a large number of requests). In the latter case, if a user sends a large number of revocation checking requests for different certificates during a short period of time, CRG will add the user's IP address into a blacklisting. CRG could be configured to ignore traffic from that IP or reject that traffic.

c) Communication Intercepting and Hijacking Attacks

As illustrated in Figure 3, we introduced a certificate DB in CRG to query and update the certificate revocation status. If attackers are able to monitor the communication with this certificate DB, they can launch a man-in-the-middle attack by intercepting messages and modifying the revocation status in Step 3a and Step 5b, respectively. In order to ensure the confidentiality and integrity of each request, we use authenticated encryption (using symmetric keys) to build a secure channel between CRG and the external DB.

If attackers manage to have malicious access to CRG, in particular to the communication channel between the certificate modifier and the client, they can hijack and modify the certificate response in Step 6 of Figure 3. Here, we can distinguish two scenarios in the context of modifying the response in Step 6. First, an attacker can modify a fake certificate with a legitimate one. This scenario brings down the security to that of the traditional infrastructure, where no revocation check is performed. In the second scenario, we assume that an attacker modifies a legitimate certificate with a fake one. We can overcome the issue in such a scenario by setting up an entity that should be responsible for keeping track of the count of fake certificates sent to the client. A System Administrator could be alerted if the count of fake certificates is more than a certain limit. Devising a sophisticated mechanism for dealing with such a scenario is part of our future work.

Unless the context clearly requires otherwise, throughout the description, the words "comprise", "comprising", and the like, are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense, that is to say, in the sense of "including, but not limited to".

Although this invention has been described by way of example and with reference to possible embodiments thereof, it is to be understood that modifications or improvements may be made thereto without departing from the scope of the invention. The invention may also be said broadly to consist in the parts, elements and features referred to or indicated in the specification of the application, individually or collectively, in any or all combinations of two or more of said parts, elements or features. Furthermore, where reference has been

made to specific components or integers of the invention having known equivalents, then such equivalents are herein incorporated as if individually set forth.

Any discussion of the prior art throughout the specification should in no way be considered as an admission that such prior art is widely known or forms part of common general knowledge in the field.

CLAIMS

1. A certificate revocation system for checking the validity of digital certificates in a secure online channel where there is a certificate authority capable of issuing a digital certificate to an application server, the application server capable of communicating the digital certificate to a client, the system comprising:

a) a certificate checker to intercept a certificate message from the application server to the client and to forward a certificate revocation request to a certificate validator,
b) a certificate validator to check the status of the digital certificate in the certificate message with the revocation manager,
c) and when said status returns “valid” a certificate modifier sends a validated certificate to the client,
d) and when said status returns “revoked” a certificate modifier sends a fake certificate to the client, such that validation at the client will fail.

2. A certificate revocation system of claim 1 wherein the certificate checker intercepts the certificate message, the certificate checker consults the certificate database before forwarding a certificate revocation request to a certificate validator.

3. A certificate revocation system of claim 1 or claim 2 wherein the system includes caching the returned statuses, either “valid” or “revoked” in a certificate database.

4. A certificate revocation system of claim 1, 2 or 3 wherein the certificate validator requests the certificate status, obtains the status and sends the response to the certificate checker.

5. A certificate revocation system of any one of the previous claims wherein the certificate checker updates the certificate database and forwards the decision together with the digital certificate to the certificate modifier, which can send the original or fake certificate to the client.

6. A certificate revocation system of any one of the previous claims wherein at interception of the certificate message by the certificate checker the certificate checker extracts the serial number of the digital certificate.

7. A certificate revocation system of any one of claims 1 to 6 wherein when the certificate modifier creates a fake certificate, the fake certificate is a modified version of the original digital certificate.

8. A certificate revocation system of any one of claims 1 to 7 wherein the fake certificate is a precomputed fake certificate stored at the certificate modifier.

9. A certificate revocation system as herein described with reference to the drawings.

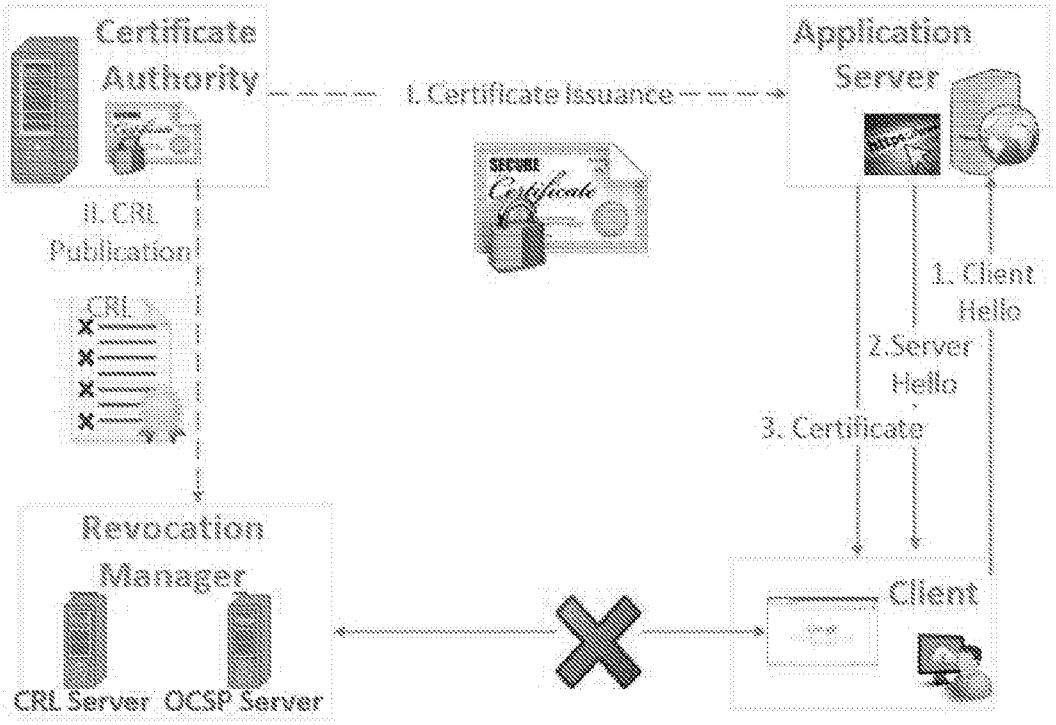

Figure 1 (Prior Art)

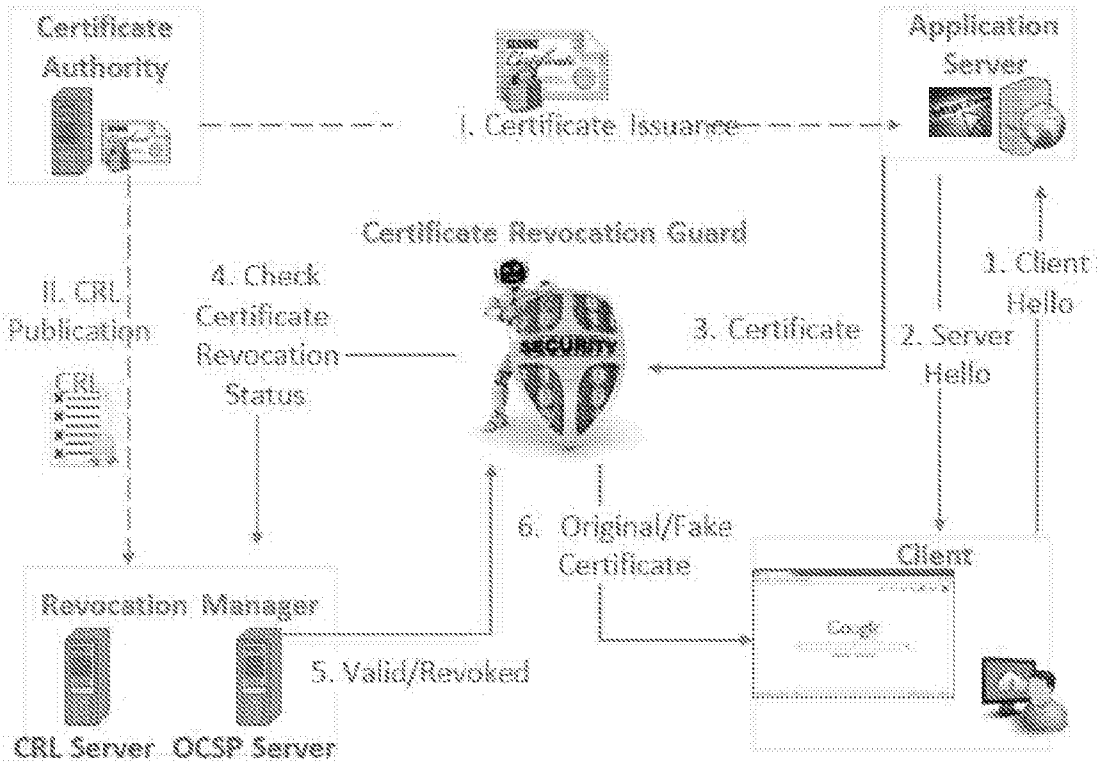
Certificate Authority
1. Certificate Issuance
Application Server
Certificate Revocation Guard
II. CRL Publication
4. Check Certificate Revocation Status
3. Certificate
2. Server Hello
1. Client Hello
CRL
SECURITY
6. Original/Fake Certificate
Client
Revocation Manager
5. Valid/Revoked
CRL Server
OCSP Server

Figure 2

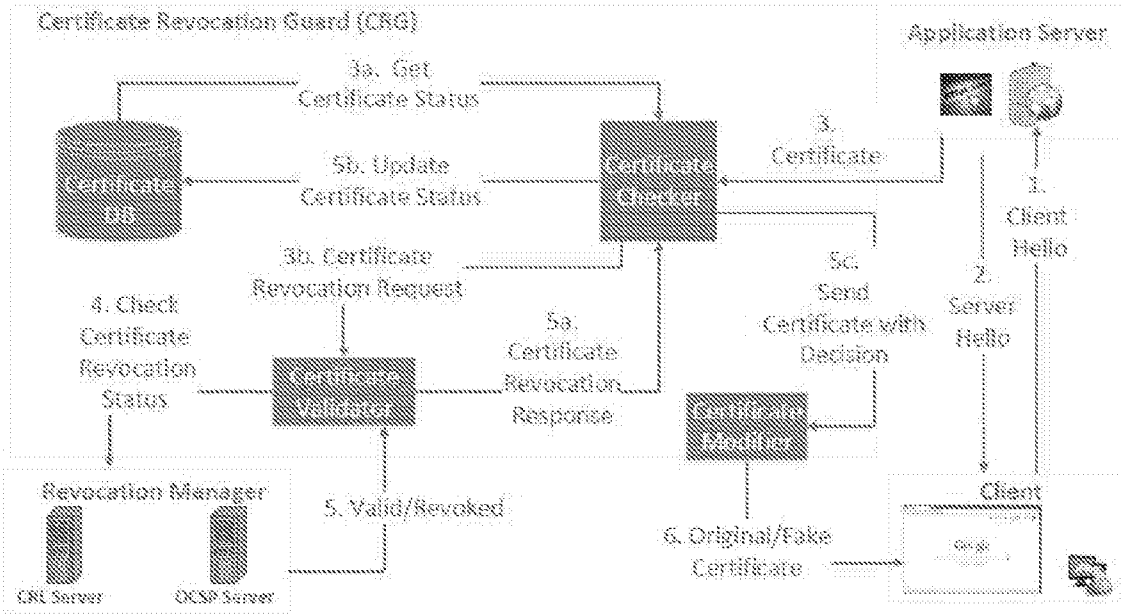

Figure 3

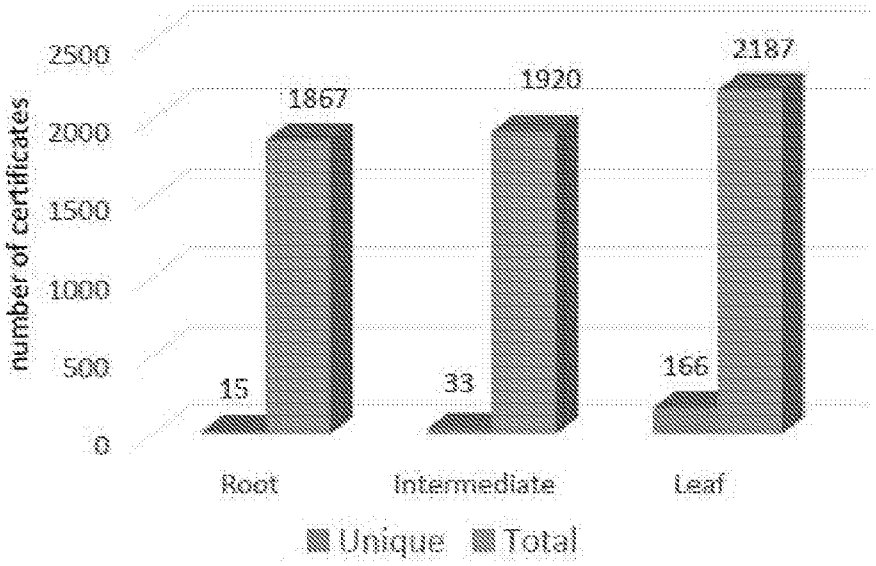

Figure 4

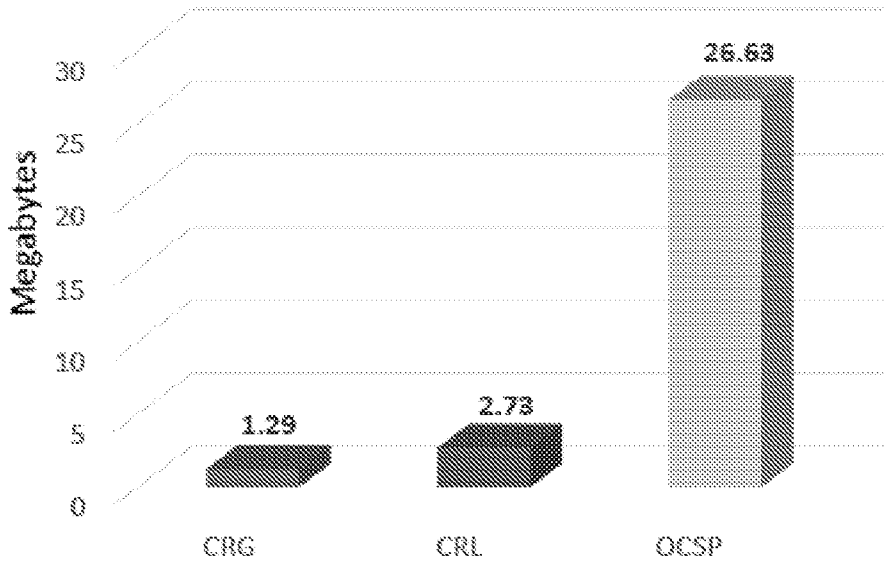

Figure 5

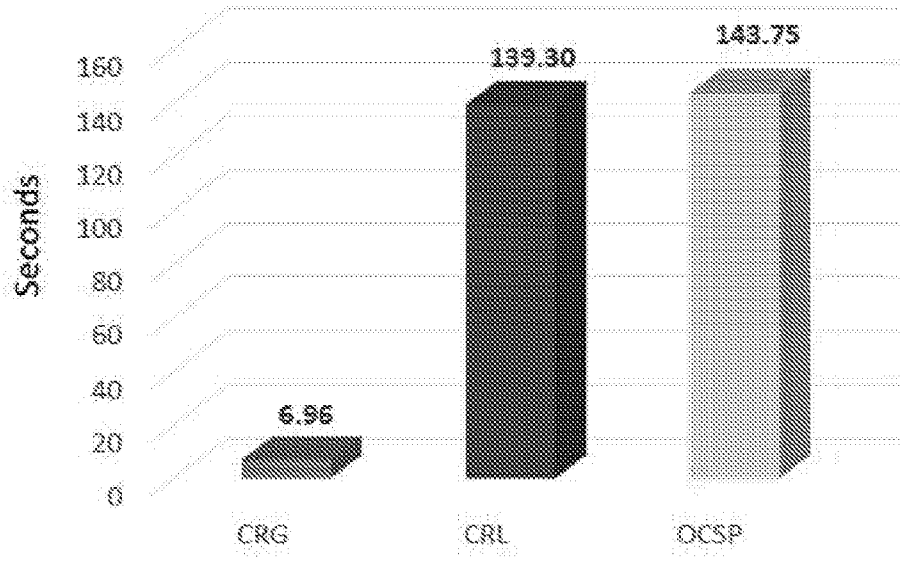

Figure 6

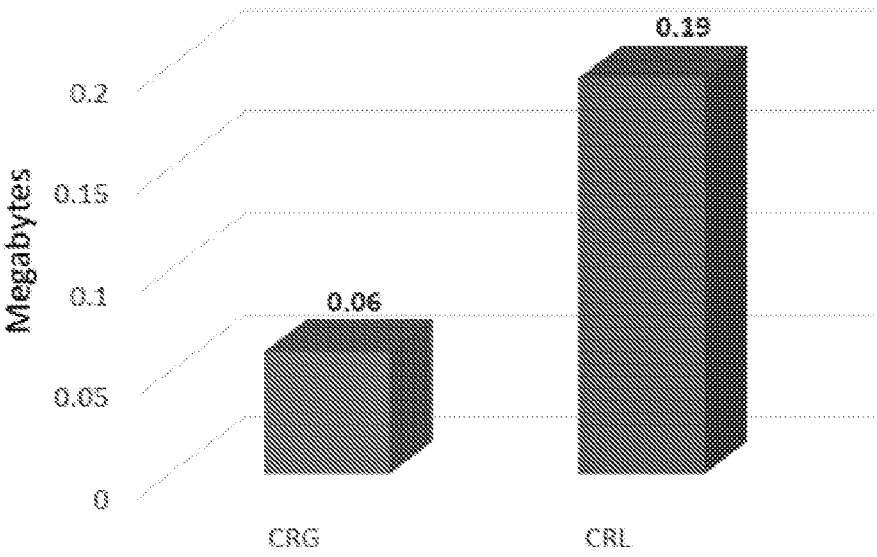

Figure 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ2017/050108

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) H04L 9/32 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Internal databases, AUSPAT and Espacenet search for applicant and inventor names.

Google Scholar/Web/Patents search with keywords and classifications [H04L63/0823, certificate revocation management, SSL, OCSP stapling, (OCSP | CRL) proxy , (faked | forged | substitute | adulterated) certificate] and similar terms.

PATENW database search with IPC marks H04L63, G06F21, G06F17 and lower and keywords [TLS, CRL, certificate revocation, OCSP, X.509, certificate authority, TLS proxy, transparent proxy, intercept, fake certificate] and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 December 2017	18 December 2017
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Marthinus Van Der Westhuizen AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262832283

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/NZ2017/050108**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/060202 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION et al.) 30 June 2005 Title, abstract; fig.5; pg.8.ln.16-25, pg.11.ln.21-26, pg.14.ln.10-17	1-8
X	US 2016/0119374 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 28 April 2016 Title, abstract; par.0037-0043	1-8
X	US 2013/0097656 A1 (KENNEDY) 18 April 2013 Title, abstract; claim 1; fig.1; par.0004-0013	1-8
X	US 2006/0143700 A1 (HERRMANN) 29 June 2006 Title, abstract; fig.5,6B; par.0011	1-8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ2017/050108

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. ☐ Claims Nos.:

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☒ Claims Nos: 9

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/NZ2017/050108**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		**Patent Family Member/s**	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
WO 2005/060202 A1	30 June 2005	WO 2005060202 A1	30 Jun 2005
US 2016/0119374 A1	28 April 2016	US 2016119374 A1	28 Apr 2016
US 2013/0097656 A1	18 April 2013	US 2013097656 A1	18 Apr 2013
		US 2015180904 A1	25 Jun 2015
		US 9231983 B2	05 Jan 2016
US 2006/0143700 A1	29 June 2006	US 2006143700 A1	29 Jun 2006
		US 7627896 B2	01 Dec 2009

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.